CERT-MU AD-2016-11

MULTIPLE VULNERABILITIES IN CISCO PRODUCTS

Original Issue Date: 03 November 2016

Severity Rating: High

Overview:

Multiple vulnerabilities have been identified in Cisco Products. These vulnerabilities could be exploited by remote attackers to cause denial of service condition, execute arbitrary code, bypass security controls on the target system, Granted full administrator privileges, cause the target system to reload, obtain full control of the system and cause a buffer overflow condition on the affected system. Cisco has issued updates and workaround(s) to address these vulnerabilities.

Description:

Multiple vulnerabilities have been identified in Cisco Products. These vulnerabilities could be exploited by remote attackers to cause denial of service condition, execute arbitrary code, bypass security controls on the target system, Granted full administrator privileges, cause the target system to reload, obtain full control of the system and cause a buffer overflow condition on an affected system.

The vulnerabilities reported are as follows:

- A vulnerability has been identified in the Slowpath of StarOS for Cisco ASR 5500 Series routers with Data Processing Card 2 (DPC2).This vulnerability exists due to improper processing during the handoff of reassembled IPv4 or IPv6 packets. This vulnerability allow an attacker to send crafted IPv4 or IPv6 fragments across the ASR 5500 Series router. On successful exploitation of this vulnerability, an unauthenticated remote attacker can cause a subset of the subscriber sessions to be disconnected, resulting in a partial denial of service (DoS) condition.

- A vulnerability has been identified in Cisco Meeting Server and Meeting App. The vulnerability exists because the software does not perform sufficient boundary checks on user-supplied data. This vulnerability allows an unauthenticated, remote attacker to send crafted IPv6 input to the vulnerable function. A successful exploitation of this vulnerability could result in an exploitable buffer underflow condition. An attacker could leverage this buffer underflow condition to incorrectly allocate memory and cause a reload of the device or execute arbitrary code with the privileges of the affected application.

- A vulnerability has been identified in the Session Description Protocol (SDP) parser of Cisco Meeting Server. The vulnerability exists because the affected software performs incomplete input validation of the size of media lines in session descriptions. This vulnerability allows an attacker to send crafted packets to the SDP parser on an affected system. A successful exploitation of this vulnerability could allow the attacker to cause a buffer overflow condition on an affected system, which could allow the attacker to execute arbitrary code on the system.

- A vulnerability has been identified in the web-based graphical user interface (GUI) of Cisco Prime Home. The vulnerability exists due to a processing error in the role-based access control (RBAC) of URLs. This vulnerability allows an attacker to send a crafted HTTP request to a particular URL
  A successful exploitation of this vulnerability could allow the attacker to obtain a valid session identifier for an arbitrary user, which would allow the attacker to perform any actions in Cisco Prime Home for which that user is authorized—including users with administrator privileges.

- A vulnerability has been identified in the content filtering functionality of Cisco AsyncOS Software for Cisco Email Security Appliances. The vulnerability exists due to incorrect validation of protected or encrypted email attachments that are Roshal Archive (RAR) format files. This vulnerability allows an attacker to send an email message that has a crafted RAR file attachment through an affected device. A successful exploitation of this vulnerability could allow the attacker to bypass content filters that are configured to detect and act upon protected or encrypted email attachments.

- A vulnerability has been identified in the Cisco Nexus 9000 Series Platform Leaf Switches for Application Centric Infrastructure (ACI). The vulnerability exists due

to improper handling of a type of Layer 2 control plane traffic. This vulnerability allows an attacker to send crafted traffic to a host behind a leaf switch. A successful exploitation of this vulnerability could allow the attacker to cause a DoS condition on the affected device.

- A vulnerability has been identified in the Transaction Language 1 (TL1) code of Cisco ASR 900 Series routers. The vulnerability exists because the affected software performs incomplete bounds checks on input data. This vulnerability allows an attacker to send a malicious request to the TL1 port, which could cause the device to reload. A successful exploitation of this vulnerability could allow the attacker to execute arbitrary code and obtain full control of the system or cause the affected system to reload.

- A vulnerability has been identified in Cisco TelePresence endpoints running either CE or TC software. The vulnerability exists due to incomplete input sanitization of some commands. This vulnerability allows an attacker to execute local shell commands with commands injected as parameters. A successful exploitation of this vulnerability could allow the attacker to retrieve full information from the device including private keys.

Impact of the attack(s)

Remote attackers can:

- Cause denial of service conditions
- Execute arbitrary code
- Bypass security controls on the target system
- Granted full administrator privileges
- Cause the target system to reload
- obtain full control of the system
- cause a buffer overflow condition on an affected system

Affected System:

- Cisco ASR 5500 devices with Data Processing Card 2 (DPC2) running StarOS 18.0 or later.
- Cisco Meeting Server releases prior to 2.0.1
- Acano Server releases prior to 1.8.16 and prior to 1.9.3
- Cisco Meeting App releases prior to 1.9.8
- Acano Meeting Apps releases prior to 1.8.35

- Cisco Meeting Server releases prior to Release 2.0.3
- Acano Server releases 1.9.x prior to Release 1.9.5
- Acano Server releases 1.8.x prior to Release 1.8.17
- Cisco Prime Home versions 5.1.1.6 and earlier and 5.2.2.2 and earlier
- All releases prior to the first fixed release of Cisco AsyncOS Software for Cisco Email Security Appliances, both virtual and hardware appliances
- Cisco Nexus 9000 Series Leaf Switches (TOR) - ACI Mode and Cisco Application Policy Infrastructure Controller (APIC).
- Cisco ASR 900 Series Aggregation Services Routers (ASR902, ASR903, and ASR907)
- All TelePresence endpoints running CE or TC software prior to first fix

CVE Information:

CVE-2016-6455
CVE-2016-6447
CVE-2016-6448
CVE-2016-6452
CVE-2016-6458
CVE-2016-6457
CVE-2016-6441
CVE-2016-6459

Solution

Users are advised to apply updates.
More information about the updates is available on:

References:

Security Tracker

http://securitytracker.com/id/1037180
http://securitytracker.com/id/1037181
http://securitytracker.com/id/1037182
http://securitytracker.com/id/1037179

Cisco

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-asr
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-cms
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-cms1
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-cph
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-esa
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-n9kapic
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-tl1
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161102-tp

Cisco Security Advisories and Alerts

https://tools.cisco.com/security/center/publicationListing.x

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. Please note that the members who do not want to receive the security alert, can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.ncb.mu
Incident: incident@cert.ncb.mu
Website: http://cert-mu.org.mu